

Claims

- [c1] 1.A method comprising:
- creating an enterprise policy object providing an enterprise-wide policy governing at least one of resource access and protocol use for a plurality of nodes within a networking environment organized within a plurality of arrays;
 - creating at least one array policy object, each array policy object providing an array-wide policy governing resource access for one or more of the plurality of nodes organized within a corresponding array;
 - and,
 - for each of one or more of the at least one array policy object, inheriting the enterprise-wide policy as the array-wide policy such that the array-wide policy of each array policy object is at least initially set to the enterprise-wide policy.
- [c2] 2.The method of claim 1, wherein the enterprise-wide policy includes a plurality of enterprise rules, each enterprise rule governing at least one of access to a particular resource and use of a particular protocol, each enterprise rule having a rule type selected from a positive rule type and a negative rule type, the positive rule type explicitly allowing at least one of access and use and the negative rule type explicitly denying at least one of access and use.
- [c3] 3.The method of claim 2, wherein each array-wide policy includes a plurality of array rules at least initially equal to the plurality of enterprise rules upon the enterprise-wide policy inherited as each array-wide policy.
- [c4] 4.The method of claim 3, further comprising, for a requested access via a requested protocol by a node organized within one of the plurality of arrays, applying the array-wide policy of the policy object corresponding to the one of the plurality of arrays to determine whether to allow the requested access via the requested protocol, such that the requested access via the requested protocol is allowed only where the requested

access via the requested protocol is explicitly allowed by the plurality of rules and not explicitly denied by the plurality of rules;
allowing the requested access via the requested protocol in response to determining that the requested access via the requested protocol is allowed; and,
denying the requested access via the requested protocol in response to determining that the requested access via the requested protocol is not allowed.

- [c5] 5.The method of claim 1, further comprising, for each of one or more of the at least one array policy object, adjusting the array-wide policy after the array-wide policy has inherited the enterprise-wide policy.
- [c6] 6.The method of claim 5, wherein
the enterprise-wide policy includes a plurality of enterprise rules, each enterprise rule governing at least one of access to a particular resource and use of a particular protocol, each enterprise rule having a rule type selected from a positive rule type and a negative rule type, the positive rule type explicitly allowing at least one of access and use and the negative rule type explicitly denying at least one of access and use;
and,
each array-wide policy includes a plurality of array rules, the plurality of array rules at least initially equal to the plurality of enterprise rules upon the enterprise-wide policy inherited as each array-wide policy.
- [c7] 7.The method of claim 6, wherein adjusting the array-wide policy comprises adding one or more new array rules to the plurality of array rules, each of the new array rules having a negative rule type explicitly denying one of access to a particular resource and use of a particular protocol.
- [c8] 8.The method of claim 7, further comprising, for a requested access via a requested protocol by a node organized within one of the plurality of arrays,
applying the array-wide policy of the policy object corresponding to the one of the plurality of arrays to determine whether to allow the

requested access via the requested protocol, such that the requested access via the requested protocol is allowed only where the requested access via the requested protocol is explicitly allowed by the plurality of rules and not explicitly denied by the plurality of rules; allowing the requested access via the requested protocol in response to determining that the requested access via the requested protocol is allowed; and, denying the requested access via the requested protocol in response to determining that the requested access via the requested protocol is not allowed.

[c9] 9.A computer-readable medium having stored thereon a computer program executable by a processor to perform the method of claim 1.

[c10] 10.A method comprising:
creating an enterprise policy object providing an enterprise-wide policy governing resource access for a plurality of nodes within a networking environment organized within a plurality of arrays;
creating at least one array policy object, each array policy object providing an array-wide policy governing resource access for one or more of the plurality of nodes organized within a corresponding array;
for each array policy object, inheriting the enterprise-wide policy as the array-wide policy such that the array-wide policy of each array policy object is initially set to the enterprise-wide policy; and,
for each of one or more of the at least one array policy object, adjusting the array-wide policy after the array-wide policy has inherited the enterprise-wide policy.

[c11] 11.The method of claim 10, wherein
the enterprise-wide policy includes a plurality of enterprise rules, each enterprise rule governing at least one of access to a particular resource and use of a particular protocol, each enterprise rule having a rule type selected from a positive rule type and a negative rule type, the positive

rule type explicitly allowing at least one of access and use and the negative rule type explicitly denying at least one of access and use; and,
each array-wide policy includes a plurality of array rules, the plurality of array rules initially equal to the plurality of enterprise rules upon the enterprise-wide policy inherited as each array-wide policy.

- [c12] 12.The method of claim 11, wherein adjusting the array-wide policy comprises adding one or more new array rules to the plurality of array rules, each of the new array rules having the negative rule type.

- [c13] 13.The method of claim 12, further comprising, for a requested access via a requested protocol by a node organized within one of the plurality of arrays, applying the array-wide policy of the policy object corresponding to the one of the plurality of arrays to determine whether to allow the requested access via the requested protocol, such that the requested access via the requested protocol is allowed only where the requested access via the requested protocol is explicitly allowed by the plurality of rules and not explicitly denied by the plurality of rules; allowing the requested access via the requested protocol in response to determining that the requested access via the requested protocol is allowed; and, denying the requested access via the requested protocol in response to determining that the requested access via the requested protocol is not allowed.

- [c14] 14.A computer-readable medium having stored thereon a computer program executable by a processor to perform the method of claim 10.

- [c15] 15.A system for governing resource access among a plurality of nodes within a networking environment, at least one or more of the plurality of nodes organized within a plurality of arrays, the system comprising:
an enterprise-policy object providing an enterprise-wide policy governing resource access for nodes organized within at least one or

more of the plurality of arrays; and,
at least one array policy object, each array policy object providing an array-wide policy governing resource access for nodes organized within a corresponding array, one or more of the at least one array policy object inheriting the enterprise-wide policy as the array-wide policy such that the array-wide policy is at least initially set to the enterprise-wide policy.

- [c16] 16.The system of claim 15, wherein the enterprise-wide policy includes a plurality of enterprise rules, each enterprise rule governing at least one of access to a particular resource and use of a particular protocol, each enterprise rule having a rule type selected from a positive rule type and a negative rule type, the positive rule type explicitly allowing at least one of access and use and the negative rule type explicitly denying at least one of access and use.
- [c17] 17.The system of claim 16, wherein the array-wide policy provided by each of the one or more of the at least one array policy object includes a plurality of array rules at least initially equal to the plurality of enterprise rules upon the enterprise-wide policy inherited as each array-wide policy.
- [c18] 18.The system of claim 17, wherein the array-wide policy provided by each of the one or more of the at least one array policy object further includes one or more other array rules, each of the one or more other array rules having the negative rule type.
- [c19] 19.The system of claim 15, wherein the array-wide policy provided by each of the at least one array policy object other than the one or more of the at least one array policy object inheriting the enterprise-wide policy does not inherit the enterprise-wide policy.
- [c20] 20.The system of claim 19, wherein
the enterprise-wide policy includes a plurality of enterprise rules, each enterprise rule governing at least one of access to a particular resource

and use of a particular protocol, each enterprise rule having a rule type selected from a positive rule type and a negative rule type, the positive rule type explicitly allowing at least one of access and use and the negative rule type explicitly denying at least one of access and use; the array-wide policy provided by each of the one or more of the at least one array policy object includes a plurality of first array rules at least initially equal to the plurality of enterprise rules upon the enterprise-wide policy inherited as each array-wide policy; and, the array-wide policy provided by each of the at least one array policy object other than the one or more of the at least one array policy object inheriting the enterprise-wide policy includes a plurality of second array rules not initially equal to the plurality of enterprise rules, each second array rule having a rule type selected from the positive rule type and the negative rule type.

- [c21] 21.The system of claim 20, wherein the array-wide policy provided by each of the one or more of the at least one array policy object further includes one or more other first array rules, each of the one or more other first array rules having the negative rule type.
- [c22] 22.The system of claim 15, further comprising at least one node policy object, each node policy object providing a node policy governing resource access for a corresponding node of the plurality of nodes other than the one or more of the plurality of nodes organized within the plurality of arrays.
- [c23] 23.The system of claim 22, wherein the node policy includes a plurality of node rules, each node rule governing at least one of access to a particular resource and use of a particular protocol, each node rule having a rule type selected from a positive rule type and a negative rule type, the positive rule type explicitly allowing at least one of access and use and the negative rule type explicitly denying at least one of access and use.